Blockchain Fog-based scheme for identity authentication in smart building

Alexander A. Varfolomeev ^{a,b} *and Liwa H. Al-Farhani* ^{b*}

^a*Bauman Moscow State Technical University, Moscow, Russia.*
^b*System Analysis, Control and Information Processing Department, Academy of Engineering, RUDN University, Moscow, Russia.*

ARTICLE INFO

ABSTRACT

This paper presents a proposal for an authentication scheme for smart building systems and environments based on blockchain, its positive features, and fog computing. The most important feature that can be distinguished in the submitted proposal is its adoption of the principle of decentralization in contrast to traditional centralized documentation protocols, i.e. the proposed authentication system in which users and smart devices are implemented in a distributed and decentralized manner on the blockchain, that will provide a solution to a significant problem of low overall efficiency of the authentication process caused by a bottleneck in such important areas as computing capacity as well as centralized storage of a single authentication authority in the traditional model. There are also benefits from adding fog computing, and because it has higher computing and storage capabilities, it makes the data processing process more efficient, faster, more streamlined, and in line with the common necessities of the real-time IoT environment. The proposed scheme also provides solutions to protect the privacy of user data and increase the level of confidentiality, protection, and security since a mysterious extractor was used to increase the confidentiality of the proposed model of the authentication system. Comparing a set of security schemes and conducting a security and performance analysis of the proposed scheme, the comparisons showed that the scheme can be characterized as having a good security level and an important efficiency level. The paper focused on specific aspects of the design of the authentication system, such as the registration and authentication process of all network entities, regardless of the specifics of the implementation of blockchain smart contracts.

1. Introduction

A technologically advanced urban setting known as a "smart city" employs numerous electronic techniques, sound activation techniques, and sensors to gather certain data. The knowledge generated from such data is utilized to manage resources, services, and assets effectively; in turn, this knowledge is used to enhance operations across the city [1].

This comprises information gathered from people, gadgets, structures, and assets that are then processed and analyzed to monitor and manage water supply and waste networks, power plants, utilities, schools, libraries, hospitals, and other community services [2]. Smart cities use technology effectively in planning, monitoring, analyzing, and administrating the city

---

* Corresponding author.
  E-mail address: *liwarussia@gmail.com* (Liwa Al-Farhani)

[3]. In order to establish a connection between the devices in the system earlier, we used cloud computing, which had emerged as a hurricane in the computing world because it supports its users in many ways, such as by lowering the project cost, backing up the information, and connecting the automotive software to hardware devices [4]. As the devices operating on the virtual world's edge get smarter and more efficient, they continuously capture information to ease human life. However, there are certain drawbacks to cloud computing, including concerns with privileges and connections across machines [5]. We employ fog computing to solve the aforementioned issues. This redistributed system, also known as fogging or the fog network is close to the end user so that it can provide data to them more quickly and with less latency [6]. Applications are shared between the cloud and the data source; it offers storage, data, and computing. It can quickly convey the information to the end user [7]. Fog computing reduces the amount of data that must be transferred to the cloud for analysis and storage. Fog computing is a more sophisticated form of cloud computing [8]. It gets around all the problems and restrictions of cloud computing. It is a distributed system between the user and the cloud, providing the user with the information they need more quickly than the cloud [9].

The main contributions of this part are presenting a proposal for a decentralized authentication system for smart buildings through fog nodes and blockchain-based smart contracts to verify and validate user access to the smart device. The proposal is based on a special blockchain base for building a network model that can further improve efficiency because the acceptance and licensing mechanisms can be described as strict to join members and reduce network consensus time. The proposal is based on two stages of audit, so this method can be considered more suitable for high-importance smart buildings that are intended to be protected from intrusions. This part also includes an explanation of the mechanics of testing and analyzing the system's efficiency to show its efficiency according to network scenarios. This part presents solutions based on distributed distribution schemes away from centralized documentation using blockchain. Taking into account, meet such important characteristics as real-time and scalability of the Internet of Things. The proposed scheme allows fog nodes and introduces a special dependence on the fuzzy extractor and the public key technique to achieve the username. As for the user's information, that information is transmitted in a non-plain text way through the channel.

Undoubtedly, IoT is one of the important technologies that are beginning to take an important place in the daily life of citizens at the level of work, home, enterprise, and public services [10]. Among the applications that belong to IoT, the smart building and the smart home are some of the important areas of these technologies nowadays. Smart buildings, according to their types and purpose, include many devices that have been automated in a smart environment that interact for a specific service and application and, as a result, lead to an improvement in the living environment [11]. The process of improving the living environment and enhancing the quality of services comes within the IoT environment

through the integration and interaction of many devices, which may be heterogeneous, but in their interaction, we can get a smarter environment and a more powerful quality of life. In this kind of smart environment, the main problems that are always referred to are security problems, hacking attempts, and problems that violate privacy [12].

There are many security problems, but the authentication problem remains a critical point in the IoT environment within smart building applications. Before going into it, we must clarify what the authentication process means. It is simply a protocol procedure that allows a specific device to be authenticated and integrates with a group of other devices within a smart environment to provide a specific service [13]. The same procedure includes the authentication of devices and users as well. That is, it is simply the actions that must be available to allow an entity to communicate with the environment as a whole. There are many common ways to perform authentication, including password-based and other biometric information-based, most of which require a trusted third party to complete the authentication steps [14]. Centralized solutions that adopt a structure based on a reliable entity and a third party with a pivotal decision were the prevailing solutions before the emergence of the blockchain and its expansion as a new technology through which work is being done to improve the security environment in smart buildings [15]. Fog nodes and blockchain are developing as an integrated way to create authentication systems in smart buildings. Several attempts have emerged, many of which are based on blockchain and cloud nodes and provide within the general IoT environment a reference model, a framework, and security mechanisms for conducting the authentication process [16].

An authentication system combining fog nodes and blockchain has also been proposed where each fog node in the IoT environment has a specific job of managing a set of devices in the smart building. Through a mechanism through which both the fog node and the smart device, as well as all entities participating in the system, can use a dedicated interface for registration and authentication to access Ethernet smart contracts, and therefore, when these contracts are executed, they lead to the completion of users' authentication on the blockchain and their registration [17].

2. System model

Network model: In the smart building, there is a special environment containing dozens of multi-use and multi-purpose smart devices and fog nodes. These nodes cooperate to serve stand-alone applications or achieve certain services within the smart home. Therefore, there must be a secure and reliable process for this cooperation, and to achieve this secure authentication, the proposal introduces a system based on the blockchain and special fog nodes. The short form of the network for the smart building environment consists of participants, a reliable authority (RA), end users, fog nodes, and various smart devices so that Ethernet smart contracts are distributed and cover all parts of the private blockchain network. The computing and storage capabilities of IoT devices are modest, or it can be said limited, so the smart building network deploys local miners. RA is

considered a reliable third party with high computing capabilities and larger storage volumes if it is responsible for configuring some of the required security variables in the network. The role of local miners is to fill contact data in the blockchain specifically in transactions that are attached to the blockchain [18]. It is called the administrator or System Manager (SM). The role of this node as a verification node can be summarized to significantly reduce the participation of each node compared to the compatibility time of the public blockchain network and also has a role in satisfying the real-time nature of the IoT system. Although the blockchain network being introduced is a private network, the decentralization feature is what distinguishes this proposal.

The registration process is carried out on the private blockchain network for all fog devices as well as smart devices to become able to connect. The process of following specific rules is also carried out after registration to set some devices to hold fog near them. Besides, the important information generated during the system setup will also be populated on the blockchain. Thus, the process of registering all fog entities and smart devices on the network is carried out, and the blockchain carries out the authentication process.

The end user in the smart building has computing capabilities and resources that can be described as good and sufficient to access and operate smart contracts because the process begins with a request from the user wishing to communicate with the smart device in the smart building, he requests permission from the smart contract to access a specific smart device and sends the user an authentication request that triggers the smart contract and when this user is granted access, he connects to the fog node that is nearby and is responsible for managing the selected smart device for authentication. As for the smart contract, the proposal presented here for the authentication system given the authentication process before access between the user and the device includes the operation of the smart contract if the requirements for its operation are completed.

Threat model: In this part and within the proposal presented, the authentication method is based on the use of the widely used Dolev-Yao Threat Model. According to the assumptions of this model, communication between any two parties through an insecure channel means that they are unreliable and that the process is unreliable, as the information used for registration and authentication can be confidential or the information itself can be modified, distorted, and changed. The details are described as:

o The hypothesis is that an attacker can penetrate some smart building devices and extract important information from those devices to be used for authentication and registration.

o The premise is that RA is a completely reliable step and that the information that is generated in RA or by a method is impenetrable and tamper-proof.

o The presented method assumes that the registration stage sends its data via a reliable and secure channel, while the authentication stage via an open channel is not secured.

o We also assume that the fog node is a reliable entity that acts as an intermediate stage during the authentication of the end-user on the smart

device. If the fog node is hacked, it means that the entire network is at risk. It has tamper-resistant specifications and capabilities, and all the data that exists in the fog nodes, whether for impersonation or authentication, is secured.

3. Proposed scheme

According to the proposed solution, the proposed authentication includes three stages that can be summarized as follows:

Pre-Configuration Phase: It is an initialization stage specific to RA and is a pre-configuration process of authentication-related variables for all entities, whether for nodes or smart devices that grow to the network. Simply put, this part is mainly for RA to ensure configuration preparations for everyone, whether it is fog nodes or smart devices in the smart building, as follows:

o RA performs an identity calculation for each of the entities belonging to the network since it is obvious that each entity smart device or fog that has a unique media access control (MAC) address on the Internet by using a hash function to hash the *MAC* address to find the entity's identity $ID_i=Hash$ (MAC_i). The hash string will be sent to all network participants for storage, where the smart device is labeled as SM_{ID} while the fog is labeled as F_{ID}.

o RA generates a pair of public and private keys (P_K and PR_K) for all entities participating in the network that will later be used in authentication processes to identify the integrity and validity of the user.

o It is also taken into account that there is a prior distribution of devices according to the fog nodes due to pre-defined mapping basics.

o The fog node computes the token *Request* of every smart device for the following phase of registration, which includes the F_{ID} of the fog node that controls the desired smart device, the SM_{ID} of that smart device, and also includes the signature result using the Elliptic Curve Digital Signature Algorithm (ECDSA). The signature is signed by using the fog node private key.

o All this information is saved in the form of blocks of transactions where, after the network consensus process is completed, it is attached to the end of the blockchain.

Registration Phase: This is the second stage, which includes the process of registering all entities, i.e. all smart devices and fog nodes in the blockchain, in turn, end users also register in RA, where their data is stored, which is stored as transactions. The network topology is formed through the process of registering nodes and smart devices in it, and the allocation is logical, where there is a link between the identity information of smart devices and the fog nodes to which they belong, and therefore, the hardware information is stored in the form of transactions on the blockchain. At this stage, the process of registering all entities participating in the network, i.e. smart devices, fog nodes, and users, is carried out using a secure and secure channel from hacking.

Table 1. Algorithm 1 of registration

Begin
   if(MAC$_{FID}$ == true)
     if(!exist(F$_{ID}$))
       if(h(MAC$_{FID}$) == F$_{ID}$)
        Completion of registration.
       end if
     end if
   end if
End

Fog Node Registration: This stage takes the following steps:

o All steps are in the form of transactions, so the fog node submits a registration transaction request, and it is sent to the system that runs the smart contract and then runs the corresponding registration verification process.

QueRegister(MACF$_{ID}$,F$_{ID}$)

o Upon receipt of the request, RA inquires if the node has been registered based on the identity of the fog node if this is achieved, the request is rejected.

o After that, the reliability of the F$_{ID}$ is checked through to the media access control address where the registration is completed if it is correct, or if it is not correct, the registration is refused

o After the registration process is completed, the fog node is accepted to join the blockchain as a full-fledged independent node. The specific registration process for the fog node is shown in Algorithm 1.

Smart Device Registration: According to the network, each fog node is connected to a group of smart devices, so when a new but shared smart device is registered, the information of this device must be available in addition to the information of the fog node to which it is connected. In the same way as before, a registration request is sent as a transaction to the blockchain that runs the smart contract and begins verification procedures.

QueRegister(MACFID,FID,MACSID,SID,RequestFID,PkSID)

The specific steps are as follows:

o A verification process is carried out whether the smart device is already registered; if it is registered, the new registration request is stopped, and this step is performed by RA**.**

o The verification of the device and the corresponding fog node, as well as the MAC address, is carried out and also verifies in the registration request the S$_{ID}$ and F$_{ID}$ correctness by the MAC address.

o Based on the smart device identity token, ***RequestF$_{ID}$*** verified PF$_K$, S$_{ID,}$ and F$_{ID}$ in the registration request. The smart device will add and accept the request to join the blockchain if all the above steps are achieved. But if no step is achieved, the request is rejected.

User Registration: Any user of this network, before communicating with any device, must log in to RA, and here the cell phone ***SIM*** card is relied on as part of the registration requirements, as follows:

o Each user must select a unique identity ***ID$_i$*** and a password *CW$_i$* and also use the biological information like fingerprint ***FG*** at the mobile device.

o Based on fuzzy extractor generator function G( ), ***Pi*** generates two types of strings, the first is a secret string ***S*** and the second is an auxiliary string ***A*** will not be used in the next steps.

G(FG) →(S, A)

o Smartphones use ***FG*** to protect the password (***CWi=h(CW$_i$∥s)***); after that, the mobile device sends the request of registration {***ID$_i$, CW$_i$, A***} to *RA* through the secure channel.

o RA used the received data in the request message to calculate a pseudo-identity ***PS$_i$=h(ID$_i$∥A)***. The *RA* configures a message of reply {***PS$_i$***} to ***SIM,*** *and* the information of this user (***PS$_i$,*** **A**) will be stored in the blockchain for use in the next process of authentication, which includes (PS$_i$,h( ), A, G( ), R( )).

o When the user receives the response from RA, he saves all the information to his memory.

Authentication Phase: This stage includes the two-factor authentication process between users and smart devices in the network before these end users can communicate with those devices. Before the communication between end-users and smart devices, it is necessary to establish a secure channel between them through two-way authentications. In our proposed scheme, a fog node manages a group of smart devices. Therefore, during the authentication process, the end-user does not directly interact with the corresponding smart device but mutually authenticates with the fog node that manages the smart device. When a user wants to access a smart device, the user *Ui* first enters his identity *ID$_i$* and password *CW$_i$*. At the mobile *SIM*, the user presses his fingerprint *FG* on the cell phone screen, and the cell phone calculates:

*R(FG,A)→S**

CW=h(IDi∥S*)*

If ***CWi=CW**** the user logs in successfully using the fuzzy extractor embedded init. Then the mobile terminal submits the authentication request transaction event.

Auth (IDi,CWi,SID)

To the local blockchain, and then triggers the smart contract deployed on the blockchain to execute the authentication process on the chain and the authentication is carried out according to the following steps:

1. Detection step: It is the first step that represents the process of

verifying the identity of the user who requested to communicate with one of the devices in the network PS_i, and this is done based on the information about that user previously stored on the blockchain. In case there is alias identity information for that user, we proceed to the second detection process related to the media access address $MACS_{ID}$, if it is saved, the detection process is completed, and we proceed to continue the query process in the next step.

2. After that, it is checked whether the device is located inside the smart building network, or is a thoughtless request, and this is done by querying SID from the blockchain, as it retains all the details where it is searched for, if it exists, as well as the MAC for the device and continuing with the following steps, but if it does not exist, it means exiting the verification process.

3. Relying on the smart contract deployed on the network's blockchain, which leads to the return of a message with:

Access= (TOKEN, A, PSi, FID, T1, ΔT))

This message reaches all members of the network of users, as well as fog nodes, which is broadcast by the blockchain and contains the following information:

TOKEN=h (SID||PSi||SID)

TOKEN is produced by hashing PS_i, F_{ID}, and S_{ID}. T_I it is the time of the current session.

4. When this message is received, which was broadcast by the blockchain, the end user starts the procedures and steps of the authentication process outside the chain and performs another verification process whether the new condition :

Tnew-T1<ΔT

5. At this step, the user authenticates himself by sending a message to the responsible fog node of the corresponding smart device:

{B1，Sign (B1),PKuser}

Where: $B1= (TOKEN,A,PS_i,T_2,N,PK_{user},ΔT)$, N is a random number, *Sign* ($B1$) is it is a digital signature phrase that is produced by the end-user based on the end user's key.

6. In this step, The role of the fog node comes in the following:
   o It is the turn of the fog node to use the user's private key to perform the detection process and, verify the authenticity of the signature first, and then verify whether the following condition is met or not.

Tnew-T2<ΔT

o The fog node is also conducting another verification process to confirm whether the identity PS_i sent by the user is the same as that sent via the broadcast, but if it is uneven, the authentication process is terminated.

o It is also verified by the fog node about the token provided by the user for the purpose of authentication whether he is correct or not.

o The fog node compute:

TOKEN=h (SID||FID||PSi)*

o A comparison process between **TOKEN** and **TOKEN*** to determine whether it is equal, the authentication process will continue or unequal, and the authentication process ends.

o After that, a response message is sent from the fog node responsible for managing the device to be communicated with by the user to the end user, which includes :

{M2, Sign (M2),PkFID}

Where: M2= (n-1, T3, PkF_{ID}), Sign (M2) it is the digital signature produced by the fog node based on its private key owned by each node.

7. The last step is the responsibility of the end user who requested authentication after receiving the message from the fog node by doing several roles:

o The process now becomes reversed, where the user performs a signature verification process depending on the public key of the fog node that sent the message and is responsible for the desired smart device.

o The user also checks whether the below condition is met or not, where it terminates the operation if the condition is not met.

Tnew-T3<ΔT

In the final result, the Secure Connection is established normally between the user and the required smart device referred to as Step No. 9 in Fig.1 and the data exchange process takes place, as Fig.1 shows the sequence of steps between the network components according to the proposed solution to the final result.

8. After that, a final encryption and decryption process is carried out, which includes an additional security step, the purpose of which is to protect the smart building from access by malicious users or subversive purposes.
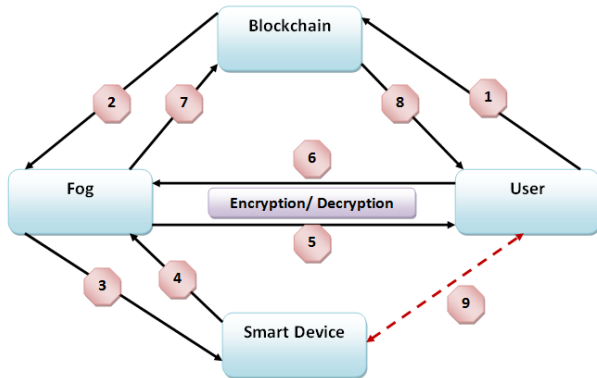
Figure 1: Sequence of authentication steps according to the proposal

4. Security analysis and performance evaluation

This section represents the process of analyzing the solutions provided in accordance with our methodology proposed in this chapter, where the security requirements of the general IoT environment will be clarified and the security aspect of the proposed authentication system for the smart building will be analyzed, and at the end, the performance evaluation of the proposed work methodology will be reviewed. It is worth noting that the security requirements in the smart building environment and the Internet of Things environment that can be adopted to evaluate the proposed performance are confidentiality, integrity, tamper resistance, and mutual authentication, which any new proposal must meet to be effective.

Security Issues Analysis: The process of designing an authentication scheme, adapting the expected security standards and requirements, and analyzing the expected problems is an essential step to ensure the reliability of services and safe and efficient operation in the smart home.

Confidentiality: Confidentiality is that users who do not comply with the terms of communication are prevented from accessing smart devices or any of the saved data and that no information belonging to users can be accessed. The process of encrypting and decrypting various data in the Internet of things can be considered a common practice that involves the implementation of a high number of key tasks based on the implementation of user authentication, which leads to the exploitation of high storage spaces as the number of users and devices in the smart building increases. In the authentication scheme proposed in this part, it is computationally illogical for an attacker to attempt to obtain *MAC* addresses from fog nodes and smart devices by deduction where the fog node, *MAC* addresses of the smart device, and the resulting sequence string from the execution of a one-way function are used as a unique identifier. Also, the role of fuzzy extractor prevents there from being any benefit from any information that can be obtained during the correspondence because it adopts pseudonyms, and therefore personal information cannot be used and will not be valid either.

Scalability: Each fog node in the smart building is associated with a set of devices according to the proposed network format. When there is a need to replace or add new devices, direct interaction with the predetermined nearby node is possible. Registration and authentication requests are

executed in a distributed way on the blockchain, which leads to support, especially the desired scalability requirement.

Integrity and Tamper-proof: One of the most important standards of the IoT environment is data integrity and tamper resistance, which leads to data protection and Prevention of leakage or illegal modification, and any proposed authentication system must be able to detect such cases and avoid their occurrence. In the proposed work methodology for the presented scheme, the solution is based on a blockchain that deals with data in the form of blocks of transactions to be stored, and all authentication and registration steps are events through which smart contracts are triggered by a transaction-based workflow. The blockchain enjoys possibilities as a secure technology that prevents data manipulation and high-level business transparency so that none of the stored blocks can be tampered with, only with the knowledge of everyone involved in the network. There is also another security stage through testing the sent messages to ensure the integrity of the data in the registration and authentication using digital signatures, and the keys for each fog node are used for encryption associated with the registration process. Depending on the public key, it is possible to detect any tampering that has obtained data within the content of the message used for registration when decryption is performed.

During the authentication phase, if the message is $M1=(TOKEN, A, PS_i, T2,n, Pk_{user}, \Delta T)$, then the subsequent authentication process will be terminated, so the suggested scheme presents a good data integrity level.

Non-repudiation: This standard is to ensure the innocence of any step taken by any of the parties to the exchange of information on the network. The presence of a private and public key in the submitted blister makes it difficult for him to disavow the step that is happening, as the user must use his private key at any step and the receiver uses the public key to verify the transmitted information easily. The blockchain also implements all the steps in the form of events, transactions, and smart nodes that are saved in the form of blocks in the blockchain with the sending party and the receiving party in an irrevocable way

Mutual authentication: This is the need to prove the identity and status before directly exchanging data or using official interaction between the parties. The proposal includes that in the case of communication between the user and any smart device belonging to the network, interaction is carried out first with the fog nodes to which the device to be communicated belongs, and a mutual authentication process is carried out using a smart contract, and therefore all these details are stored with authentication variables and their certificate on the blockchain. In other words, the proposed authentication protocol includes an important step: when the end user within the smart building network requests a smart device, the fog node is communicated through a message broadcast back from the blockchain. The fog node sends a reply message, which is an $\{M2, Sign (M2), PkF_{ID}\}$ to complete authentication to the other party, and these steps realize the concept of two-way authentication.

Privacy and anonymity: Undoubtedly, it is one of the most important criteria by which any new proposals and solutions can be evaluated, as privacy, identity preservation, and private information are among the red

standards that must be observed at all steps, as in the event of any information leakage, this leads to unimaginable problems. The proposed scheme guarantees the complete confidentiality of all information exchanged during its three stages so that no information related to the end user is disclosed because the steps in registration and authentication use a series extracted from the biometric information of the user as a protective substitute for the real identity of that user with the use of a pseudonym when sending. Since, according to the proposal, at the authentication stage, the real name of the user is not used, but a fake name is used in the process of interception or hacking, it is impossible to know the true identity of the user, i.e. the proposed scheme provides a high level of guarantee for privacy, user data and anonymity. By reviewing the analysis of some of the common threats and security problems that IoT systems are exposed to in general, the proposal should provide solutions, guarantees, and the ability to overcome these problems to be reliable.

Message substitution attack: The authentication scheme in this part is based on blockchain, and the relevant information of each participant has been written into the distributed ledger at the beginning of initialization. It is not possible to replace or change information at the registration stage so that the registration transaction request is submitted to the private key signature of the blockchain, and the entire verification process is performed on the blockchain and all of them are saved as blocks in the blockchain. Also at the authentication stage, there are two stages of authentication, the first is on-chain and the second is off-chain, as an on-chain process in which information cannot be replaced, but for off-chain authentication, the end user receives *access,* after which M1 is sent with attachments representing a signature that is built and created using the key data of that end user. The same mechanism is used in the response of the fog node, so the replacement of information is impossible and not possible.

Sybil attack and spoofy attack: However, the proposal presented in the authentication form proposes the principle that each smart device has a unique S_{ID} that is used to identify that smart device. The same applies to the fog nodes that have a unique F_{ID} that distinguishes them from others, and the user does not deal with his real identity, but with a PS_i pseudonym or a unique alias as well, and all this information turns into blocks stored in the blockchain, so the hypothesis of impersonation or the creation of fake identities is not possible. The proposal also includes steps that expose fake activity or any attempt to do so, where users need to authenticate with each other on the blockchain before interacting with a smart device, which prevents the attacker from impersonating a legitimate user to communicate with other devices, as this step requires verification of the unique identity of the end user and the unique identity of the fog node, and thus impersonation of other entities by the attacker is difficult or impossible.

Replay attack: After the registration process is completed by the devices, the fog nodes and users create unique identities for each of them that are stored on the blockchain. Also, time stamping is essential for all messages sent during the authentication phase, as they are time-stamped, i.e. any messages that are restarted will be exposed due to time stamping, which leads to the rejection of their operation when the smart contract is

authenticated, i.e. there are no ideal conditions for an adversary or an attacker to carry out this type of Replay attacks

Man in the middle (MITM): This type of attack occurs when there is the possibility of intercepting data sent through the network during interaction processes, communication between different devices or between fog nodes and users, where the sent messages include timestamp Ti data during the interaction between the end user and the fog node, as it also includes the sender's private key, which is a fundamental pillar of mutual authentication. This means that the attacker does not have access to the private keys of these interacting parties, which leads to preventing the possibility of launching a man-in-the-middle attack.

Denial of service (DoS): It is a type of malicious attack that relies on the principle of sending a large number of request messages to a specific service provider during a certain period not to obtain the service, but to overload the system, which leads to the announcement of the inability to respond and thus bring down that system. The schemes proposed here, which are based on the blockchain, imply the existence of a special local blockchain to which all participating entities belong, and therefore everyone is subject to a special blockchain access mechanism, which is carried out only through the administrator's registration verification process to be able to join the blockchain. Also, joining the blockchain, the role of the local administrator is important in the packaging and deployment of blocks, which prevents synchronization per unit of time, that is, he cannot start large-scale requests in a short period. Table 2 shows the process of comparing the proposed solution according to the analysis we presented above for each of the points with the authentication system proposed by us in this chapter.

Table 2: Security comparison with other current schemes

Confidentiality	[19]	[20]	[21]	This work
Scalability	N	N	N	Y
Integrity	Y	Y	N	Y
Tamper-Proof	Y	Y	Y	Y
Mutual Authentication	Y	Y	N	Y
Decentralization	Y	Y	Y	Y
Sybil	Y	Y	N	Y
Message Substitution	N	Y	N	Y
Spoof	Y	Y	Y	Y
Message Reply	Y	Y	Y	Y
MITM	Y	Y	Y	Y
DoS	Y	Y	N	Y

Performance Evaluation: The purpose of using fog nodes in the scheme proposed in this part for blockchain-based authentication is to provide a set of services for localized computing of the entire network in a way that goes beyond the frequency of sending data to the cloud for no processing purpose in each round, which in turn contributes to reducing latency. Farthermore, as was explained earlier, the fog nodes in the smart building are added to the blockchain so that they are responsible for a group of smart devices scattered at home and connected to that fog node, and this also leads to counting the existence of an obligation or compulsion for users to search

for the corresponding device to communicate with the smart device where they can authenticate by communicating with the fog node that manages the required smart device. Since the authentication process is decentralized on the blockchain and is an essential feature of the blockchain, the authentication authority and its procedures. Since the authentication process is decentralized on the blockchain, the authority to complete the authentication consists of multiple fog nodes, which contributes to a clear increase in the productivity of the proposed system. The smart devices in the Internet of things have limited computing power and storage capacities, so they are considered light nodes when they are inserted into the system, on the contrary, fog nodes have higher computing and storage capabilities. For this reason, the storage of data and related information in the collective Ledger during the authentication process is in the fog nodes due to their storage capabilities. In this part of the chapter, we review a detailed analysis of each stage of the proposed authentication scheme by knowing the cost of communication and general accounting expenses to evaluate whether the proposal meets the desired standards and requirements or not, taking into account the absence of a fixed reference object considered as a standard for an authentication system in a smart building so that we can compare with it.

Communication Overhead: Here we quantify the total number of bits of messages exchanged in the authentication scheme to represent the communication overheads of our scheme. Table 3 illustrates the values used in the proposal.

Table 3: Assumed values

Length Of Identity	128 bits
Length of Pseudo-Identity	128 bits
Length of Output Of Fuzzy Extractor	128 bits
Length of Random Numbers	128 bits
Length of Timestamp	32 bits
Hash Function	SHA-256 algorithm
Signature Algorithm	ECDSA algorithm
Length Of Public And Private Keys	128bits

The communication overhead of the smart device, the user, and the fog node is mainly affected by the messaging process during registration and authentication, as shown in Fig. 3 and 4. These figures show that the smart device during the registration stage has the highest communication cost associated with it for a good reason because it needs the information of the corresponding fog node simultaneously with sending it. Since authentication is a large part of the process that takes place in the blockchain, this part does not appear in the form and comparison, where most messages are associated with the user, so the cost of communication is the highest for him at the authentication stage.
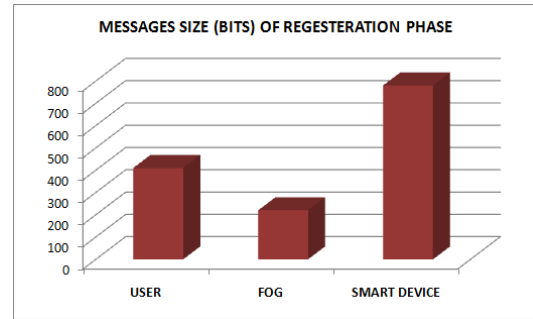
Figure 3: Comparison of message sizes transmitted in the registration phase
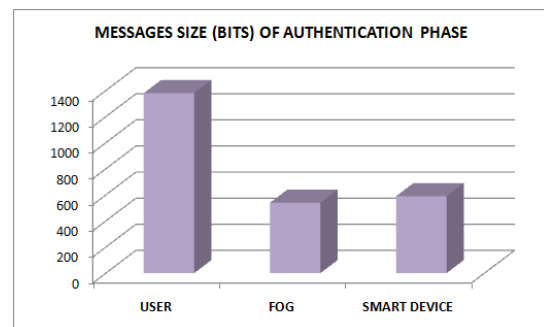
Figure 4: Comparison of message sizes transmitted in the authentication phase

Computation Analysis: In the proposed scheme, the largest percentage of the calculation occurs at the configuration stage in terms of implementation so that the RA performs all hashing operations to calculate all the identities of entities in the network and then initialize the variables for that and initiate the process of assigning pairs of public and private keys to all these entities within the network. The smart device is not strongly involved during the implementation of the entire authentication protocol, and it does not need to perform many operations such as encryption, hashing, as well as signing, this is the description of the placement of smart devices in the overall smart building environment because they have limitations in computational capabilities as well as limited storage capacities.

According to these limited capabilities that smart devices have in the smart home, their investment is limited and limited to what can be implemented with these capabilities from reasonable and simple steps, but complex steps that require computing and storage capacities higher than the capabilities of smart devices are processed and carried out in the fog nodes or end users That is, each group of smart devices managed by fog nodes transfers its complex processes to the fog layer of the network to invest computing power, so the complex processes of fog nodes and end users are left to solve, achieving a rational allocation of computing resources. To evaluate the proposed scheme, it is initially the process of calculating the total execution times of the encrypted primitives that are used in the scheme to calculate the total computational cost and then compare. Initially, it should be clarified what the following abbreviations mean where denote the computation time of hash function (T_h), denote the computation time of

fuzzy extractor (T_f) denote the computation time of message encryption and decryption (T_{ed}), denote the computation time of ECC point multiplication (T_e), denote the computation time of message authentication code (T_{mac}) and denote the computation time of hash MAC respectively (T_{hamc}). Based on the simulation results of [22], which will used to denote the average time for sending a request of authentication to the blockchain and message exchange in terms of T_{req}, T_{exc}. It is also assumed that there is an approximate equivalence between the runtime of the message authentication code, the hash message authentication code, as well as the hash function, and here there is another assumption that $T_h=T_{hamc}$. Table 3 explains the times of execution of the primitives of cryptographic:

Table 3: Approximate running time of cryptographic primitives

Operation	Computaiton cost (ms)
Hash Function(T_h)	0.0052
Message authentication code(T_{mac})	0.0052
Hash MAC(T_{hamc})	0.0052
Symmetric encryption/decryption(T_{ed})	0.0215
Fuzzy extractor Gen/Rep(T_f)	0.4276
ECC point multiplication(T_e)	0.4276
Generate request in BC(T_{req})	1.0690
Generate data message(T_{exc})	0.0300

In this chapter, we proposed an authentication method for smart buildings based on the role of fog nodes, where the authentication process is divided into on-chain and off-chain authentication processes. An authentication on-chain that starts from submitting an authentication request to the smart contract to return an authentication code, depending on the cost of calculations per paragraph shown in Table 3, the computational cost of this type of authentication is:

$T_{req}+T_{exc}=1.069+0.03=1.099\ ms$

The second type, which represents off-chain authentication steps the computational cost, is:

$3*T_h=3*0.0052= 0.0156\ ms$

Table 4: Comparison of computation costs

Scheme	Total computation cost	ms
[23]	$2T_{ed}+3T_h$	0.06380
[24]	$4T_{ed} + T_f+22T_h$	0.05120
[25]	$18T_h+ 10T_E$	0.06176
[22]	$3T_{ed}+ T_{req}+T_{exc}$	1.16350
[26]	$T_{req}+T_{exc}+3T_h$	1.11460
This work	$T_{req}+T_{exc}+3T_h+2T_{ed}$	1.15760

And since there is a final stage in which there is a double protection process through the process of encryption and decryption, which consumes:

$2* T_{ed} = 2*0.0215=0.043\ ms$

The total computation cost of the proposed scheme = 1.1576 ms. Table 4 also reflects the clear difference between solutions based on centralization and solutions based on decentralization, which relies on the participation of everyone without any reliable authority. This third party has the right to decisive decisions. On the one hand, the centralized method gives quick solutions, but compared to the problems of a single point of failure, security vulnerabilities, as well as lack of transparency, the possibility of changing files without the user's knowledge, and other disadvantages of centralized methods, the choice falls on the developer based on the importance and sensitivity of the application.

5. Conclusion

The main contributions of this part are presenting a proposal for a decentralized authentication system for smart buildings through fog nodes and blockchain-based smart contracts to verify and validate user access to the smart device. The proposal is based on a special blockchain base for building a network model that can further improve efficiency because the acceptance and licensing mechanisms can be described as strict to join members and reduce network consensus time. The proposal is based on two audit stages, so this method can be considered more suitable for high-importance smart buildings that are intended to be protected from intrusions. The proposed scheme also provides solutions to protect the privacy of user data and increase the level of confidentiality, protection, and security since a mysterious extractor was used to increase the confidentiality of the proposed model of the authentication system. Comparing a set of security schemes and conducting a security and performance analysis of the proposed scheme, the comparisons showed that the scheme can be characterized as having a good security level and an important efficiency level. The part focused on specific aspects of the design of the authentication system, such as the registration and authentication process of all network entities, regardless of the specifics of the implementation of blockchain smart contracts. Therefore, the future development of this work should include delving into the details of the consensus mechanism of the blockchain network to ensure the integrity and logic of the certified data as taken for granted in this part to achieve a higher level of optimization than the proposed authentication scheme.

Authors' contribution
All authors contributed equally to the preparation of this article.

Declaration of competing interest
The authors declare no conflicts of interest.

References

[1] S. P. Mohanty, U. Choppali and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," in IEEE Consumer Electronics Magazine, vol. 5, no. 3, pp. 60-70, July 2016. doi: 10.1109/MCE.2556879.

[2] Moura F., de Abreu e Silva J.," Smart Cities: Definitions, Evolution of the Concept and Examples of Initiatives," In Leal Filho, W., Azul, A., Brandli, L., Özuyar, P., Wall, T. (eds) Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer, Cham. 2019.

[3] Moch N., Wereda W.," Smart Security in the Smart City, " Sustainability 2020, 12, 9900, 2020. https://doi.org/10.3390/su12239900.

[4] Araujo, V., Mitra, K., Saguna, S., Ahlund, C.," Performance evaluation of FIWARE: A cloud-based IoT platform for smart cities," Journal of Parallel and Distributed Computing, vol.132, pp.250-261,2019.

[5] Alam T.," Cloud-Based IoT Applications and Their Roles in Smart Cities," Smart Cities, vol.4, pp.1196-1219, 2021.

[6] C. M. Kanaka Sri Shalini, Y. M. Roopa and J. S. Devi, "Fog Computing for Smart Cities," International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 912-916, 2019. doi: 10.1109/ICCES45898.9002050.

[7] M. K. Saroa and R. Aron, "Fog Computing and Its Role in Development of Smart Applications," IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, VIC, Australia, pp. 1120-1127, 2018, doi: 10.1109/BDCloud.2018.00166.

[8] Javadzadeh, G., Rahmani, A.M. Fog Computing Applications in Smart Cities: A Systematic Survey. Wireless Netw, vol. 26, pp. 1433–1457, 2020.

[9] M. M. Kamruzzaman, Bingxin Yan, Md Nazirul Islam Sarker, Omar Alruwaili, Min Wu, Ibrahim Alrashdi, "Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities", Journal of Healthcare Engineering, 2022.

[10] Fotohi R.; Shams Aliee F.," Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," Comput. Netw. vol. 197, 2021.

[11] M. M. Kamruzzaman et al., "Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities," Journal of Healthcare Engineering, 2022.

[12] I. P. Naria, S. Sulistyo and Widyawan, "Security and Privacy Issue in the Internet of Things, Smart Building System: A Review," International Symposium on Information Technology and Digital Innovation (ISITDI), Padang, Indonesia, pp. 177-180, 2022.

[13] Bashir, M.R., Gill, A.Q. & Beydoun, G.," Reference Architecture for IoT-Enabled Smart Buildings," SN COMPUT. SCI. 3, vol. 493 ,2022.

[14] A. Aslesha and A. Sivanesh Kumar, "An Improved Integrated Solution for Novel Home Security System with various Force Points using BYOD," 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, pp. 828-831, 2022, doi: 10.1109/ICOSEC54921.2022.9951959.

[15] Singh P., Nayyar A., Kaur A. Ghosh U.," Blockchain and Fog Based Architecture for the Internet of Everything in Smart Cities," vol. 12, 61,2020, https://doi.org/10.3390/fi12040061.

[16] Alzoubi Y.I., Gill A. & Mishra A.," A systematic review of the purposes of blockchain and fog computing integration: classification and open issues," J Cloud Comp 11, vol. 80, 2022, https://doi.org/10.1186/s13677-022-00353-y.

[17] H. H. Al Oliwi, Z. A. Husain and R. Rafeh, "Integrating Blockchain and Internet of Things for Smart Homes," Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, pp. 77-82, 2021. doi: 10.1109/ComComAp53641.9652936.

[18] Heshmati, A., Bayat, M., Doostari, M. et al.," Blockchain-based authentication and access verification scheme in smart home," J Ambient Intell Human Comput,2022.

[19] R. Al madhoun, M. Kasha, M. Alhemeiri, M. Alshehhi and K. Salah, "A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes," IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8, 2018.

[20] Z. Cui et al., "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241-251, 1 March-April 2020.

[21] M. Wazid, A. K. Das, V. Odelu, N. Kumar and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 391-406, 1 March-April 2020.

[22] Khalid, U, Asim, M, Baker, T, C. K. Hung, P, Adnan Tariq, M. , and Rafferty, L," A Decentralized Lightweight Blockchain-based Authentication Mechanism for IoT Systems," Cluster Computing, vo. 23, pp. 2067-2087,2020.

[23] Kumar P, Gurtov A, Iinatti J, Ylianttila M, Sain M.," Lightweight and secure session-key establishment scheme in smart home environments," IEEE Sensors J, vol.16, pp.254–264, 2015.

[24] M. Wazid, A. K. Das, V. Odelu, N. Kumar and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 391-406, 1 March-April 2020.

[25] Mengxia Shuai, Nenghai Yu, Hongxia Wang, Ling Xiong, "Anonymous authentication scheme for the smart home environment with provable security", Computers & Security, vol. 86, pp. 132-146, 2019.

[26] X Xu, Y Guo, Y Guo," Fog-Enabled Private Blockchain-Based Identity Authentication Scheme for Smart Home", IEEE TRANSACTIONS ON MOBILE COMPUTING 10, Available at SSRN 4052337 - papers.ssrn.com, 2022.